IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES, Plaintiff, v. ANDREW KASNETZ, Defendant.	No. 3:18-CR-345-D

GOVERNMENT'S RESPONSE TO DEFENDANT'S OBJECTIONS TO GOVERNMENT'S EXHIBIT LIST

The United States Attorney for the Northern District of Texas, by and through the undersigned Trial Attorney, respectfully submits this response to defendant's objections to the Government's Exhibit List. The exhibits identified in the Government's Exhibit List, Doc. No. 185, are authentic, relevant, reliable, and admissible. Defendant's slipshod objections seek to resurrect the motion to suppress that this Honorable Court previously denied and invite the Court to ignore well-settled precedent involving nearly identical facts. The Court should therefore deny defendant's objections to the Government's Exhibit List.

I. Background

In 2017, the Plano Police Department conducted an investigation into the sharing of child pornography on a public peer-to-peer computer network called BitTorrent. During this investigation, law enforcement observed a device using defendant's IP address publicly sharing files known to be associated with child pornography. Investigators used this information to obtain a warrant to search defendant's residence. During the search of defendant's residence on February 20, 2018, investigators observed defendant's computer

actively downloading child pornography using BitTorrent. Investigators seized electronic devices belonging to defendant which contained tens of thousands of images and videos depicting children engaged in sexually explicit conduct. Investigators also found footage from defendant's home security camera system recorded immediately before law enforcement arrived depicting defendant in his home office completely naked and sitting in front of a computer which was actively downloading child pornography.

On April 8, 2022, the Government filed its Exhibit List, which identifies fifty-two exhibits, including:

- Four electronic devices containing child pornography seized from defendant's residence;
- Nine exhibits of images and videos of child pornography extracted from defendant's electronic devices, as described in the Superseding Indictment;
- Eighteen exhibits of digital forensic artifacts extracted from defendant's devices;
- Two home security camera videos depicting the unclothed defendant using his desktop computer minutes before the search of his residence;
- Four exhibits of screenshots depicting files and folders on defendant's devices;
- Seven exhibits of photos and videos taken during the search of defendant's residence;

- Three exhibits attributing to defendant the use of devices containing child pornography, including a trust agreement bearing defendant's name and signature;
- One video demonstrating the operation of uTorrent;
- One exhibit of basic subscriber information for defendant's internet service; and
- Three chain of custody documents.

On May 10, 2022, defendant filed objections to nearly every exhibit on the Government's Exhibit List except for a video of the inside of defendant's residence, a photograph of the exterior of the residence, a demonstrative video of uTorrent, and subscriber information for defendant's internet service. Doc. No. 204 at 2. Defendant identified four categories of objections.

In his first category, defendant claims that nearly every Government exhibit was "seized / collected pursuant to what Defendant contends was an illegal search under the 4th Amendment[.]" While defendant acknowledges that the Court denied his motions to suppress, he does not articulate any theory explaining how these exhibits were seized in violation of the Fourth Amendment nor does he cite any case excluding similar evidence.

In his second category, defendant objects to introduction of child pornography identified in the indictment and screenshots of folders of child pornography on defendant's devices. Defendant incorrectly claims that the probative value of these exhibits is substantially outweighed by danger of unfair prejudice.

Defendant's third objection relates to "[i]tems seized / collected through forensic means." Doc. No. 204 at 6. In this category, defendant appears to argue that the Government is unable to authenticate such evidence, that the Government witnesses lack personal knowledge about those exhibits, and that these exhibits contain inadmissible hearsay. Defendant does not explain this misguided objection, nor does he cite any cases holding that a trial court erred in admitting files and forensic artifacts extracted from a defendant's devices by the Government's forensic examiners.

Finally, defendant objects to admitting a trust document extracted from his electronic devices.[1] Defendant wrongly argues that this document is not relevant and contains inadmissible hearsay.

II. The Court Has Already Denied Defendant's Motion to Suppress

On March 22, 2022, the Court issued a memorandum opinion denying defendant's motion to suppress. Doc. No. 172. The Court found that the Government "establishe[d] that only publicly available information was accessed during" the investigation which initially identified defendant and that defendant "has failed to establish a Fourth Amendment violation[.]" *Id*. at 5. The Court held that investigators seized electronic devices from defendant's residence and forensically examined those devices pursuant to a valid search warrant. *Id*. at 6. The Court concluded, "Defendant's Motion and this ground for suppression are without merit and fail to establish a violation of the Fourth Amendment." *Id*.

[1] Defendant also objects to admitting tax documents found on his computer. The Government does not intend to admit these documents into evidence. Defendant's objections to these exhibits are therefore moot.

Undeterred by the Court's ruling, Defendant baldly declares that the exclusionary rule prohibits introduction of nearly all the Government's evidence. Defendant fails to cite a single case even remotely related to the trafficking of child pornography on peer-to-peer networks and does not cite any authority endorsing the type of wholesale exclusion of evidence he requests here.

The Fifth Circuit has affirmed convictions involving precisely the sort of evidence the Government intends to offer at trial.[2] In *United States v. Weast*, law enforcement observed a user share child pornography on a peer-to-peer network, discovered that user's IP address, and received a search warrant to search the residence associated with that IP address. 811 F.3d 743 (5th Cir. 2016). Investigators seized computers belonging to the defendant, forensically examined those devices, and discovered child pornography. *Id*. at 746. The Fifth Circuit held that "Weast's Fourth Amendment rights were not violated" by the seizure of such evidence from his residence. The case at bar is nearly identical to *Weast* and defendant offers no reason for this Court to depart from Fifth Circuit precedent. The Court should accordingly overrule defendant's objections to exhibits identified in "Category One" of his memorandum.

[2] The Fifth Circuit is hardly alone in affirming convictions based on similar evidence. *See*, *e.g.*, *United States v. Chiaradio*, 684 F.3d 265 (1st Cir. 2012); *United States v. Niggemann*, 881 F.3d 976 (7th Cir. 2018); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009); *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *United States v. Norman*, 448 F. App'x 895, 897 (11th Cir. 2011) (unpublished).

III. Child Pornography on Defendant's Devices Forms the Basis of the Charged Conduct and is Admissible

The Government intends to admit child pornography found on defendant's devices and publish those images and videos to the jury. These images and videos are central to the charged offenses and their probative value is of the highest order. This evidence is accordingly admissible, and the Government should be allowed to publish the images and videos to the jury.

As stated by the Fifth Circuit in *United States v. Caldwell*, "child pornography is graphic evidence that has force beyond simple linear schemes of reasoning. It comes together with the remaining evidence to form a narrative to gain momentum to support jurors' inferences regarding the defendant's guilt. It provides the flesh and blood for the jury to see the exploitation of children." 586 F.3d 338, 343 (5th Cir. 2009). The Fifth Circuit concluded that the trial court did not abuse its discretion when it showed the jury excerpts from three of the seventeen different videos of child pornography on defendant's computer. *Id*. Further, the publication of child pornography to the jury helps "establish the likelihood that the defendant knew that the video depicted child pornography." *United States v. Lampley*, 781 F. App'x 282, 285 (5th Cir. 2019).

There is broad consensus that the government may publish graphic child pornography to the jury. *See*, *e.g.*, *United States v. Perez*, 712 F. App'x 136, 141 (3d Cir. 2017); *United States v. Luck*, 852 F.3d 615, 626 (6th Cir. 2017) ("the pornographic nature of the image in a child pornography case plays a vital role in the government's narrative of the concrete events comprising the charged offense […] the images in a child pornography

prosecution have multiple utility, tending to establish both the fact that they are pornographic and the fact that defendant acquired and distributed the images knowing they depicted child pornography."); *United States v. Loughry*, 738 F.3d 166 (7th Cir. 2013); *United States v. Evans*, 802 F.3d 942 (8th Cir. 2015) (government showed the jury 14 images and 22 video clips of child pornography, which took approximately 5 minutes to show).

Defendant's reliance on *United States v. Welshans*, 892 F.3d 566, 576 (3rd Cir. 2018), is misplaced. In *Welshans*, the Third Circuit found that the probative value of child pornography depicting bestiality, bondage, and the violent sexual assault of very young children was substantially outweighed by danger of unfair prejudice where "the Government had extensive evidence that did not involve violent or sadistic content, and Welshans stipulated that the files recovered were child pornography." *Id.*[3]

The Government does not seek to introduce the type of extreme material described by the Third Circuit in *Welshans*. Moreover, the case at bar does not involve a stipulation that the images and videos on defendant's computer depicted child pornography. Here, the Government intends to meet its burden of proof by offering the files identified in the Superseding Indictment and depictions of the folders where defendant saved those files as representative samples[4] of the child pornography found on defendant's computers.

[3] It would be improper for the Court to require the Government to stipulate that the images and videos depict child pornography. Requiring such a stipulation would "rob the evidence of much of its fair and legitimate weight." *Lampley*, 781 F. App'x at 285.

[4] "[T]he use of representative samples of child pornography in these cases has been broadly upheld." *United States v. Naidoo*, 995 F.3d 367, 376 (5th Cir. 2021) ("There is no question that the pornography shown was a limited portion of the thousands of images and hundreds of videos for which Naidoo was held accountable. Moreover, it is clear that the number of images contributed to the narrative strength of the Government's case.").

In similar circumstances, the Fifth Circuit found that "such videos are of significant probative value" and their probative value is not substantially outweighed by the low danger of *unfair* prejudice. *Lampley*, 781 F. App'x at 286. The Court should accordingly overrule defendant's objections to admitting images and videos depicting child pornography.

IV. Files Extracted from Defendant's Electronic Devices are Admissible

Evidence of files extracted from defendant's computers, metadata concerning those files, reports of forensic artifacts from defendant's computers, and chain of custody documents are authentic, relevant, and meet the requirements for applicable hearsay exclusions and exceptions.

"The standard for authentication is not a burdensome one." *United States v. Jackson*, 636 F.3d 687, 692–93 (5th Cir. 2011). The proponent of an item of evidence may satisfy the authenticity requirement by producing "evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). An item of evidence may be authenticated by various means, including the testimony of a witness with knowledge, distinctive characteristics, or "[e]vidence describing a process or system and showing that it produces an accurate result." Fed. R. Evid. 901(b).

The Government intends to authenticate defendant's electronic devices through the testimony of law enforcement officers who seized defendant's computers from his residence. Law enforcement officers recorded the seizure of these devices on chain of custody documents describing each item seized, including their make, model, and serial numbers. Moreover, officers took photographs during their search of defendant's residence

showing the location and condition of each item at the time of seizure. *See United States v. Davis*, 754 F.3d 278, 281 (5th Cir. 2014) (evidence is properly authenticated where the prosecution introduces testimony accounting for how evidence came into police custody and establishing how police logged and maintained that evidence).

Next, the Government will authenticate files found on these devices through the testimony of forensic examiners who extracted the files. These witnesses will testify that they extracted files from defendant's devices using reliable and forensically sound methods commonly used in the field of digital forensics. *See* Doc. No. 202 ("Government's Memorandum Concerning Witnesses Tendered Under Fed. R. Evid. 702").

This testimony will be similar to testimony offered in *United States v. Dioubate*, where the United States District Court for the Eastern District of Texas found the same techniques to be "generally accepted in the computer industry as well as the legal community." No. 1:13-CR-40, 2013 WL 12064121, at *3 (E.D. Tex. Dec. 13, 2013) (collecting cases and agreeing with the Government's proffer that "the examinations are performed with commercial off-the-shelf software applications used industry-wide in the private sector, government agencies, and by local, state, and federal law enforcement agencies, including the Secret Service, ICE-HSI, and the Federal Bureau of Investigations ("FBI")").

Some of the files extracted from defendant's devices include reports of forensic artifacts generated by those devices. For example, Government Exhibit 30 is a report of "Jump Lists," which are computer-generated records of files and folders recently accessed by the user of defendant's desktop computer. In addition to showing that digital forensic

evidence is authentic and relevant, the Government will establish that the machine-generated data contained in those files is not hearsay because the "declarant" is defendant's computer, not a person. *See* Fed. R. Evid. 801(b) ("'Declarant' means the person who made the statement.") (emphasis added).

The Fifth Circuit has long held that such records are admissible. *See*, *e.g.*, *United States v. Fendley*, 522 F.2d 181, 187 (5th Cir. 1975) ("We do not believe, however, that computer evidence is so intrinsically unreliable as to make its introduction clear error."). Indeed, courts around the country routinely admit into evidence a wide variety of machine-generated data. *See*, *e.g.*, *United States v. Channon*, 881 F.3d 806, 811 (10th Cir. 2018) (machine-generated transaction records in Excel spreadsheets not hearsay); *United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109–10 (9th Cir. 2015) (a Google Earth "tack" placed at labeled GPS coordinates not hearsay); *United States v. Lamons*, 532 F.3d 1251, 1263–64 (11th Cir. 2008) (machine-generated data collected from calls made at airline's corporate toll-free number not hearsay statement, for Confrontation Clause purposes); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (header information generated by fax machine not a hearsay statement because it is not "uttered by 'a person' [and] nothing 'said' by a machine ... is hearsay").

Tellingly, defendant does not seriously contend that these exhibits are anything other than what they purport to be: electronic devices seized from his residence, files saved to those devices, and machine-generated artifacts found on those devices. Defendant offers no case law or other supporting documentation that cast into doubt the admissibility of

these exhibits. The Court should accordingly overrule defendant's objection to "Items seized / collected through forensic means."

V. Defendant's Trust Agreement on His Computer Establishes that He Exercised Ownership and Custody Over That Computer

"In order to obtain a conviction under 18 U.S.C. § 2252A(a)(5)(B)[], the government must prove beyond a reasonable doubt that [the defendant] knowingly possessed material that contained an image of child pornography[.]" *United States v. Moreland*, 665 F.3d 137, 149 (5th Cir. 2011). The presence of a document creating a trust for defendant on his computer tends to show that he exercised ownership and custody of that computer. Further, saving that type of information to a desktop computer shows that defendant's possession of that computer was exclusive. *Id*. at 152-154. Defendant's trust document is therefore relevant under Fed. R. Evid. 401.

Further, statements found on this document are not offered for the truth of the matter asserted and are accordingly not hearsay. The significance of this document lies not in the accuracy of the information recorded, but rather in the fact that it bears defendant's name and signature. *See* Fed. R. Evid. 801(c), advisory committee note ("If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay."). Defendant's objection to Exhibit 38 should therefore be overruled.

VI. CONCLUSION

The Court should overrule defendant's objections to the Government's Exhibit List.

Respectfully submitted,
CHAD MEACHAM
United States Attorney

/s/ Eduardo Palomo

Eduardo Palomo
Trial Attorney
Texas Bar No. 24074847
U.S. Department of Justice
1301 New York Ave. NW
Washington, D.C. 20005
Telephone: (202) 305-9635
eduardo.palomo2@usdoj.gov

CERTIFICATE OF SERVICE

I certify that on May 13, 2022, I filed this response with the clerk of court for the U.S. District Court, Northern District of Texas, which generated service to counsel for defendant.

/s/ Eduardo Palomo

Eduardo Palomo
Trial Attorney